IN THE SPECIFICATION

Please amend Page 8, Line 14 through Page 9, Line 8 to read as follows:

Fig. 1 is a function configuration diagram illustrating functions relating to ~~claim 1 according to~~ an embodiment of the invention;

Fig. 2 is a function configuration diagram illustrating functions relating to ~~claim 2 according to~~ an alternative embodiment of the invention;

Fig. 3 is a function configuration diagram illustrating functions relating to ~~claim 3 according to~~ an alternative embodiment of the invention;

Fig. 4 is a function configuration diagram illustrating functions relating to ~~claim 4 according to~~ an alternative embodiment of the invention;

Fig. 5 is a function configuration diagram illustrating functions relating to ~~claim 5 according to~~ an alternative embodiment of the invention;

Fig. 6 is a function configuration diagram illustrating functions relating to ~~claim 6 according to~~ an alternative embodiment of the invention;

Fig. 7 is a function configuration diagram illustrating functions relating to ~~claim 7 according to~~ an alternative embodiment of the invention;

Fig. 8 is a function configuration diagram illustrating functions relating to ~~claim 8 according to~~ an alternative embodiment of the invention;

Fig. 9 is a function configuration diagram illustrating functions relating to ~~claim 9 according to~~ an alternative embodiment of the invention;

Fig. 10 is a function configuration diagram illustrating functions relating to ~~claim 10 according to~~ an alternative embodiment of the invention;

Please amend Page 10, Lines 14-21 to read as follows:

Fig. [[8]] 11 is a device configuration diagram illustrating a cipher strength evaluation apparatus of this embodiment. As shown in Fig. [[8]] 11, the cipher strength evaluation apparatus is a general purpose computer, for example, having a CPU 101, an internal memory 102, an external storage 103 such as HDD, a communication interface 104 such as a modem for connecting to communication networks, a display 105, and an input unit 106 such as a mouse and a keyboard.

Please amend Page 11, Lines 11-20 to read as follows:

The estimated stirred text calculating part 12 as shown in Figures 6, 7, 8, 9, and 10 accepts plaintext satisfying a predetermined condition, calculates an estimated equivalent key estimated as an equivalent key determined from a first-step extended key being an extended key at a first step, and calculates first-step estimated stirred text satisfying a predetermined condition and estimated as stirred text at the first step based on the plaintext and the estimated equivalent key. With the use of the estimated stirred text calculating part 12 like this, the level-1 first-round elimination can be performed.

Please amend Page 12, Lines 6-14 to read as follows:

It is also possible to use an estimated plaintext calculating part 11 as shown in Figures 1, 2, 3, 4, and 5 for calculating plaintext from stirred text instead of the estimated stirred text calculating part 12 by the same operation as that of the estimated stirred text calculating part 12. Since the stirring parts of the Feistel encryption apparatus are shared to realize both functions of

encryption and decryption, the estimated plaintext calculating part 11 has the same structure as that of the estimated stirred text calculating part 12.

Please amend Page 12, Lines 15 through Page 13, Line 1 to read as follows:

The encryption control part 2 as shown in Figures 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10 uses and allows the encryption apparatus to calculate ciphertext based on the plaintext accepted by the estimated stirred text calculating part 12. It directly or indirectly inputs plaintext into the encryption apparatus operating on the same computer as that on which the cipher strength evaluation apparatus operates or on another computer through a communication interface, and allows the encryption apparatus to calculate ciphertext corresponding to the plaintext. It is acceptable to be an apparatus that communicates with a storing part having plaintext and ciphertext corresponding to the plaintext stored therein and allows ciphertext to be calculated virtually.

Please amend Page 13, Lines 2-11 to read as follows:

The last-but-one-step estimated stirred text calculating part 33 as shown in Figures 5 and 10 accepts the ciphertext calculated by the encryption control part 2, calculates a last-step estimated extended key estimated as an extended key at the last step by exhaustive search, and calculates last-but-one-step estimated stirred text estimated as stirred text at the last-but-one step being the preceding step of the last step based on the ciphertext and the last-step estimated extended key. It estimates the last-step estimated extended key by exhaustive search on the equivalent key at the seventh step.

Please amend Page 13, Lines 12-17 to read as follows:

Generally, the last-but-one-step estimated stirred text calculating part 33 can be formed to be a predetermined-step estimated stirred text calculating part 31 as shown in Figures 4 and 9 and a second predetermined-step estimated stirred text calculating part 32 as shown in Figures 2 and 7 for estimating extended keys at a plurality of steps, for example, to calculate stirred text at a given predetermined step.

Please amend Page 13, Line 18 through Page 14, Line 3 to read as follows:

The key verification part 4 as shown in Figures 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10 formulates an encryption equation with higher order differences based on the first-step estimated stirred text accepted by the estimated stirred text calculating part 12 and ciphertext calculated under the control of the encryption control part 2 or based on the last-but-one-step estimated stirred text calculated by the last-but-one-step estimated stirred text calculating part 33, processes it by an algebraic technique to try to calculate a last-but-one-step extended key or last- step extended key, and outputs a calculation impossible signal when it detects that calculation is impossible.

Please amend Page 14, Line 14 through Page 15, Line 1 to read as follows:

The decryption control part 5 as shown in Figures 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10 accepts the calculation impossible signal, controls the estimated stirred text calculating part 12, estimated plaintext calculating part 11, the encryption control part 2, the last-but-one-step estimated stirred text calculating part 33, and/or the key verification part 4 to allow the key verification part 4 or the last-but-one-step estimated stirred text calculating part 33 to calculate the last-step extended key. The decryption control part 5 outputs a recalculation request signal for requesting to

calculate an extended key until the extended key can be calculated, and then the estimated stirred text calculating part 12 or the estimated plaintext calculating part 11 and the last-but-one-step estimated stirred text calculating part 33 accept the calculation signal to recalculate each extended key.